# Reduction of Elliptic Curves in Equal Characteristic 3 (and 2)

Miyamoto, Roland; Top, Jakob

*Published in:*
Canadian Mathematical Bulletin



*Publication date:*
2005

Canad. Math. Bull. Vol. **48** (3), 2005 pp. 428–444

# Reduction of Elliptic Curves in Equal Characteristic 3 (and 2)

Roland Miyamoto and Jaap Top

*Abstract.* We determine conductor exponent, minimal discriminant and fibre type for elliptic curves over discrete valued fields of equal characteristic 3. Along the same lines, partial results are obtained in equal characteristic 2.

## 0 Introduction

This paper deals with the reduction of an elliptic curve $E$ over a discrete valued field with perfect residue field. In 1964, Néron [4] gave a complete classification of the possible types of the special fibre of a minimal proper regular model for $E$. In the tame situation, that is, in residue characteristic $\neq 2, 3$, he also characterised each fibre type in terms of the coefficients of a short Weierstrass equation for $E$. Later, Tate [11] provided an algorithm for determining the fibre type, conductor exponent and other invariants of the reduction in the general case. In 1993, Papadopoulos [6] exhibited tables for conductor and fibre type in terms of valuations and certain congruences involving the coefficients $c_4$ and $c_6$ in the cases of unequal charateristic 2 and 3.

In the present paper, we try to shortcut Tate's algorithm in the remaining cases: equal characteristic 2 and 3. This is achieved at the cost of having to compute Artin–Schreier reduced valuations inside certain explicitly given extension fields. The idea is to calculate the wild part of the conductor exponent directly from its definition and then use Ogg's Formula [5] and Néron's classification to derive the remaining invariants. As a consequence, in equal characteristic 3 we can exhibit all possible conductor exponents and reduction types for given valuation of the $j$-invariant (Section 2). In equal characteristic 2, our method seems to give slightly less precise results (Section 3). In both cases however, we have refined results due to Gekeler [2, 3] on the set of possible conductor exponents.

## 1 Preliminaries

Let us fix some notation which we shall use throughout the paper. The group of invertible elements in a ring $A$ will be denoted by $A^*$. Throughout, $K$ is a field with a discrete valuation $v$, which we assume to be normalized to $K$, that is, $v(K^*) = \mathbb{Z}$. Let $R := \{a \in K \mid v(a) \geq 0\}$ be the corresponding discrete valuation ring and $\pi \in K$

Received by the editors September 5, 2003; revised October 21, 2003.

The first author is grateful towards EAGER Benelux for funding him while preparing most of the paper. Both authors would like to thank Jasper Scholten for his valuable advice and some crucial ideas to this work.

AMS subject classification: 14H52, 14K15, 11G07, 11G05, 12J10.

a uniformizer at $v$, that is, $\pi R$ is the maximal ideal of $R$. Moreover, we assume the residue field $k := R/\pi R$ to be perfect. Once for all, we fix an extension of $v$, also denoted $v$, to the algebraic closure $\bar{K}$ of $K$. Then $v(\bar{K}^*) = \mathbb{Q}$, and the residue field of $\bar{K}$ is the algebraic closure $\bar{k}$ of $k$. All algebraic extensions of $K$ are assumed to lie in $\bar{K}$, and so their residue fields are intermediate fields of $\bar{k}|k$. For a finite field extension $L|K$, we set $v_L := e \cdot v$ where $e := (v(L^*) : v(K^*))$ is the ramification index, so that again $v_L(L^*) = \mathbb{Z}$.

## Elliptic Curves over $K$

Let $E$ be an elliptic curve over $K$ with base point $O$ and $j$-invariant $j$. As is well known, $E$ can be given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with $a_i \in K$ and discriminant $\Delta \neq 0$, such that $O = (0 : 1 : 0)$ is the intersection point of $E$ with the infinite line $z = 0$. Any two equations of the shape (1) are related by a change of variables

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t$$

with $u \in K^*$ and $r, s, t \in K$. For convenience, we abbreviate this transformation by $(u, r, s, t)$. It fixes the base point $O$ and changes the $a_i$ and $\Delta$ according to Table 1.2 in [8, p. 49]. In particular, the resulting equation has discriminant $\Delta/u^{12}$. Therefore $v(\Delta)$ is only determined by $E$ up to a multiple of 12. An equation (1) with coefficients $a_i \in R$ such that $v(\Delta)$ is as small as possible is called minimal (at $v$), and the $v$-contribution $d_v(E/K) := v(\Delta)$ to the minimal discriminant of $E$ is well-defined.

Let $\mathcal{W}/R$ be the projective scheme given by a minimal Weierstrass equation for $E$. Recall that $E$ is said to have good, resp. multiplicative, resp. additive, reduction at $v$, if the special fibre $\mathcal{W} \times_R k$ is an elliptic curve, resp. has a node, resp. has a cusp. Moreover, there always exists a finite field extension $L$ of $K$ such that $E \times_K L$ has either good or multiplicative reduction, in which case $E$ is called potentially good or potentially multiplicative, respectively. The former case occurs if and only if $v(j) \geq 0$.

In general, the scheme $\mathcal{W}$ will not be regular. But, as Néron [4] has shown, there always exists a minimal proper regular scheme $\mathcal{C}/R$ such that $\mathcal{C} \times_R K \simeq E$. Its special fibre $\tilde{\mathcal{C}} := \mathcal{C} \times_R \bar{k}$ over $\bar{k}$ is a union of distinct curves $F_1, \ldots, F_m$ over $\bar{k}$ with multiplicities $n_1, \ldots, n_m$. So it can be written as a cycle $\tilde{\mathcal{C}} = \sum_{i=1}^m n_iF_i$. Denote the number of components (without multiplicities) of the special fibre by $m_v(E/K) := m$. The combinatorial intersection type of the cycle $\tilde{\mathcal{C}}$ is called the Kodaira type of $E/K$ at $v$, and is denoted $\kappa = \kappa_v(E/K)$. Néron has classified the possible Kodaira types in general. Table 1 gives the corresponding value of $m$ for each $\kappa$.

Later on, we want to determine the possible Kodaira types for given valuation of the $j$-invariant. To this end, we define the sets

$$\mathcal{K}_\nu := \{\kappa_v(E/K) \mid E/K \text{ elliptic curve}, v(j(E)) = \nu\}$$

for every $\nu \in \mathbb{Z} \cup \{\infty\}$.

*Table 1*: Fibre types of an elliptic curve $E/K$

| $\kappa_v(E/K)$ | $\mathrm{I}_0$ | $\mathrm{I}_\nu$ | II | III | IV | $\mathrm{I}_0^*$ | $\mathrm{I}_\nu^*$ | IV* | III* | II* |
|---|---|---|---|---|---|---|---|---|---|---|
| $m_v(E/K)$ | 1 | $\nu$ | 1 | 2 | 3 | 5 | $\nu+5$ | 7 | 8 | 9 |

## Conductor Exponent

Another important invariant of $E/K$ is its conductor exponent at $v$. By definition, it is the conductor exponent of the representation of the absolute Galois group of $K$ on the Tate module $T_\ell(E)$ for any prime number $\ell \neq \operatorname{char} k$. We first recall some facts on Hilbert's ramification theory. Let $L|K$ be finite Galois with group $G := G(L|K)$, and $R_L := \{a \in L \mid v(a) \geq 0\}$. For $s \geq -1$, the $s$-th lower ramification group is defined as

$$G_s = G_s(L|K, v) := \{\sigma \in G \mid \forall a \in R_L : v_L(\sigma a - a) \geq s+1\}.$$

Obviously, this definition is stable under a change of the lower field $K$, that is, if $K'$ is an intermediate field of $L|K$ then $G_s(L|K', v) = G_s(L|K, v) \cap G(L|K')$. For compatibility with a change of the upper field, one introduces the upper ramification groups $G^{\eta(s)} = G^{\eta(s)}(L|K, v) := G_s(L|K, v)$ obtained by renumbering via the continuous bijection

$$\eta = \eta_{L|K} \colon [-1, \infty) \to [-1, \infty), \quad s \mapsto \int_0^s \frac{dx}{(G_0 : G_x)}.$$

***Proposition 1.1*** *For any Galois subextension $L'|K$ of $L|K$, the restriction map $G(L|K) \to G(L'|K)$ sends $G^t(L|K, v)$ onto $G^t(L'|K, v)$ for all $t \geq -1$.*

Note that $\eta$ is the identity on $[-1, s]$ as long as $G_s = G_0$. Moreover,

$$G_{-1} = G^{-1} = \{\sigma \in G \mid v \circ \sigma = v|_L\}$$

is the decomposition group,

$$G_0 = G^0 = \{\sigma \in G \mid \forall a \in R_L' : v(\sigma a - a) > 0\}$$

is the inertia group, and

$$G_1 = \bigcup_{t>0} G^t = \{\sigma \in G \mid \forall a \in R_L' : v(\sigma a - a) > v(a)\}$$

is the ramification group. We call $s \geq -1$ a (lower) jump of ($v$ in) $L|K$ if $G_t(L|K, v) \subsetneqq G_s(L|K, v)$ for all $t > s$. Clearly, the lower jumps are integers, and they are the arguments for which $\eta_{L|K}$ has a kink.

Now let $E/K$ be an elliptic curve, and pick a prime number $\ell \neq \operatorname{char} k$. Then $E[\ell] := E(\bar{K})[\ell]$ is an $\mathbb{F}_\ell$-vector space of dimension 2. Take $L = K(E[\ell])$ to be the

field obtained by adjoining to $K$ the coordinates of all the $\ell^2$ points in $E[\ell]$. Denote by $E[\ell]^{G_i}$ the $\mathbb{F}_\ell$-subspace fixed by $G_i = G_i(L|K, v)$. Then the conductor exponent of $E/K$ at $v$ can be defined as (*cf.* [9, p. 380])

$$f = f_v(E/K) := f^0 + f^1,$$

where

$$f^0 = f_v^0(E/K) := \begin{cases} 0 & \text{if } E \text{ has good reduction,} \\ 1 & \text{if } E \text{ has multiplicative reduction,} \\ 2 & \text{if } E \text{ has additive reduction,} \end{cases}$$

and

$$f^1 = f_v^1(E/K) := \sum_{i=1}^{\infty} \frac{\dim_{\mathbb{F}_\ell} E[\ell]/E[\ell]^{G_i}}{(G_0 : G_i)}.$$

The following facts are crucial to our discussion and can be found in [9, p. 381].

***Proposition 1.2***

(a) *The conductor exponent $f$ is an integer, and its definition is independent of the choice of the prime number $\ell \neq \operatorname{char} k$.*
(b) *If $f^0 < 2$, then $f^1 = 0$.*
(c) $f^1 \leq v(1728)$.

Note that the bound in (c) has no effect if $\operatorname{char} K = 2$ or 3. In fact, it has been shown by Gekeler [2, 3], that in these cases the conductor exponent can get arbitrarily large. In order to refine on his results later, we introduce the sets

$$\mathcal{F}_\nu := \{f_v(E/K) \mid E/K \text{ elliptic curve}, v(j(E)) = \nu\}$$

for every $\nu \in \mathbb{Z} \cup \{\infty\}$. Both $\mathcal{F}_\nu$ and $\mathcal{K}_\nu$ will turn out not to depend on the actual choice of the valued field $K$, but only on $\operatorname{char} K$ and $\operatorname{char} k$. An important fact is that the three invariants $d$, $m$ and $f$ of the reduction are related by

***Ogg's Formula*** $f_v(E/K) + m_v(E/K) = d_v(E/K) + 1$.

For a proof, see [5, 7].

## Example: The Tame Situation

To illustrate the computation of the sets $\mathcal{F}_\nu$ and $\mathcal{K}_\nu$ defined above, we now consider the tame situation, that is, we assume that $\operatorname{char} k \neq 2, 3$. We start by reviewing the known facts in this case as found, *e.g.*, in [9, p. 365].

***Theorem 1.3*** *Let $E/K$ be an elliptic curve, set $n := -v(j(E)) \in \mathbb{Z} \cup \{-\infty\}$, and define $d' \in \{0, \ldots, 11\}$ by $d' \equiv v(\Delta) \bmod 12$ where $\Delta$ is the discriminant of any Weierstrass equation for $E$. Then the invariants $d := d_v(E/K)$, $f := f_v(E/K)$, $m := m_v(E/K)$ and $\kappa := \kappa_v(E/K)$ are given by the following table.*

| | $n > 0$ | | $n \leq 0$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $d'$ | $n$ mod 12 | $(n+6)$ mod 12 | 0 | 2 | 3 | 4 | 6 | 8 | 9 | 10 |
| $d$ | $n$ | $n+6$ | 0 | 2 | 3 | 4 | 6 | 8 | 9 | 10 |
| $f$ | 1 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| $m$ | $n$ | $n+5$ | 1 | 1 | 2 | 3 | 5 | 7 | 8 | 9 |
| $\kappa$ | $\mathrm{I}_n$ | $\mathrm{I}_n^*$ | $\mathrm{I}_0$ | II | III | IV | $\mathrm{I}_0^*$ | IV$^*$ | III$^*$ | II$^*$ |

From this knowledge, the determination of the possible conductor exponents and Kodaira types is rather straightforward.

***Corollary 1.4*** *Let $\nu \in \mathbb{Z} \cup \{\infty\}$. Then*

(a) $\mathcal{F}_\nu = \{1, 2\}$ *and* $\mathcal{K}_\nu = \{\mathrm{I}_{-\nu}, \mathrm{I}_{-\nu}^*\}$ *for* $\nu < 0$.
(b) $\mathcal{F}_0 = \{0, 2\}$ *and* $\mathcal{K}_0 = \{\mathrm{I}_0, \mathrm{III}, \mathrm{I}_0^*, \mathrm{III}^*\}$.
(c) $\mathcal{F}_\nu = \{0, 2\}$ *and* $\mathcal{K}_\nu = \{\mathrm{I}_0, \mathrm{I}_0^*\}$ *for* $0 < \nu \equiv 0 \bmod 3$.
(d) $\mathcal{F}_\nu = \{2\}$ *and* $\mathcal{K}_\nu = \{\mathrm{II}, \mathrm{IV}^*\}$ *for* $0 < \nu \equiv 1 \bmod 3$.
(e) $\mathcal{F}_\nu = \{2\}$ *and* $\mathcal{K}_\nu = \{\mathrm{IV}, \mathrm{II}^*\}$ *for* $0 < \nu \equiv 2 \bmod 3$.
(f) $\mathcal{F}_\infty = \{0, 2\}$ *and* $\mathcal{K}_\infty = \{\mathrm{I}_0, \mathrm{II}, \mathrm{IV}, \mathrm{I}_0^*, \mathrm{IV}^*, \mathrm{II}^*\}$.

**Proof** We use the notation of Theorem 1.3. Clearly, $E/K$ has a Weierstrass equation $y^2 = x^3 + a_4x + a_6$ with $a_4, a_6 \in K$. Its discriminant is

$$\Delta = (c_4^3 - c_6^2)/1728 \neq 0$$

where $c_4 = -48a_4$ and $c_6 = -864a_6$. Then $j := j(E) = c_4^3/\Delta$. Assertions (a) and (f) are immediate from the theorem. Now assume $-n = \nu = v(j) \geq 0$. Then $n \equiv d' \bmod 3$, and $\kappa \in \{\mathrm{I}_0, \mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{I}_0^*, \mathrm{IV}^*, \mathrm{III}^*, \mathrm{II}^*\}$.

(b) $\nu = 0$ implies $d' \in \{0, 3, 6, 9\}$, and all these values of $d'$ can be realised, as one sees by taking $c_4/12 = -4a_4 = \pi^{d'/3}$ and $c_6 = a_6 = 0$.

(c)–(e) $\nu > 0$ means $v(c_4^3) > v(c_6^2) = v(\Delta)$, hence $d' \in \{0, 2, 4, 6, 8, 10\}$ with $\nu + d' \equiv 0 \bmod 3$. On the other hand all these values for $d'$ do occur, as one sees by taking $c_4 = \pi^{(\nu+d')/3}$ and $c_6 = \pi^{d'/2}$. ∎

## Artin–Schreier Extensions

Now suppose that $\mathrm{char}\, K = p > 0$. Denote by $\wp$ the Artin–Schreier operator on $\bar{K}$, that is, $\wp z = z^p - z$ for $z \in \bar{K}$. For any finite extension $K'$ of $K$, we consider the Artin-Schreier reduced valuation $v^{*K'}$ on $K'$ defined by

$$v^{*K'}(a) := \sup_{c \in K'} v(a - \wp c) \in \mathbb{Q} \cup \{\infty\}$$

for $a \in K'$, where we agree that the sup of an unbounded set is $\infty$. Note that $v^{*K'}$ defines an ultra-semimetric on $K'$ in that it satisfies the strong triangle inequality

$$v^{*K'}(a + b) \geq \min\{v^{*K'}(a), v^{*K'}(b)\}$$

for all $a, b \in K'$. The following proposition connects the jumps in an Artin–Schreier extension with the corresponding reduced values. Since $v_{K'}$ is again discrete, the result can be adapted to $K'$ where required.

***Proposition 1.5*** *Let $b \in K$ and $A \subseteq K$ be an additive subgroup containing $\wp K$ such that $A/\wp K$ is finite. Set $v^* := v^{*K}$ and $A_s := \{a \in A \mid v^*(a) > -s\}$. Then*

(a) *$v(b) \leq v^*(b) \in \{m \in \mathbb{Z} \mid 0 > m \not\equiv 0 \bmod p\} \cup \{0, \infty\}$. If $0 > v(b) \not\equiv 0 \bmod p$, then $v(b) = v^*(b)$.*

(b) *The field extension $L := K(\wp^{-1}A)$ is abelian over $K$ with group $G = G(L|K) \simeq (A/\wp K)^\vee$, the dual of $A/\wp K$. In this isomorphism, the upper ramification groups appear as*

$$G^s(L|K) = G(L|K(\wp^{-1}A_{s+1})) \simeq (A/A_{s+1})^\vee \quad \textit{for } -1 \leq s \leq 0,$$
$$G^s(L|K) = G(L|K(\wp^{-1}A_s)) \simeq (A/A_s)^\vee \quad \textit{for } 0 < s.$$

**Proof** (a) See [10, p. 114].

(b) For $\sigma \in G := G(L|K)$ and $u \in \wp^{-1}A$, we set $\chi_\sigma(\wp u) := \sigma(u) - u \in \mathbb{F}_p$. By Artin–Schreier Theory (that is, Kummer Theory for the operator $\wp$), the pairing $G \times A \to \mathbb{F}_p$, $(\sigma, a) \mapsto \chi_\sigma(a)$ is injective on the left and has right kernel $\wp K$. In the resulting isomorphism $G \simeq (A/\wp K)^\vee$, we clearly have

$$G(L|K(\wp^{-1}A_s)) = \{\sigma \in G \mid \chi_\sigma(A_s) = 0\} \simeq (A/A_s)^\vee$$

for every $s \geq -1$. This shows the asserted isomorphisms. For the equalities with the upper ramification groups, we shall use the proof in [10, p. 116] as resumed in [1, pp. 21ff]. Let $a \in A$, and set $K_a := K(\wp^{-1}a)$. Then we have the three equivalencies

$$a \in A_s \iff s > -v^*(a) \iff G^s(K_a|K) = 1$$

for all $s > 0$,

$$a \in A_0 \iff v^*(a) = \infty \iff G^{-1}(K_a|K) = 1,$$

and

$$a \in A_{s+1} \iff v^*(a) \geq 0 \iff v \text{ is unramified in } K_a|K$$
$$\iff G^s(K_a|K) = G^0(K_a|K) = G^1(K_a|K) = 1$$

for $-1 < s \leq 0$.

Hence, by Proposition 1.1, $G^s$ has fixed field $L^{G^s} = K(\wp^{-1}A_s)$ for $s > 0$ and $L^{G^s} = K(\wp^{-1}A_{s+1})$ for $-1 \leq s \leq 0$.

■

## 2 Equal Characteristic 3

Throughout this section, we assume that $K$ has characteristic 3.

***Theorem 2.1*** *Let $E/K$ be an elliptic curve given by a Weierstrass equation*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

*and having $j$-invariant $j := j(E)$.*

(a) *Assume $j \neq 0$. Then $a_2 \neq 0$. Choose a square root $\sqrt{j} \in \bar{K}$ and consider the field $\tilde{K} := K(\sqrt{j})$. Set $n_2 := v(a_2)$, $n := v(1/j)$, $\tilde{n} := 2v^{*\tilde{K}}(1/\sqrt{j})$, and define $d' \in \{0, \ldots, 11\}$ by $d' \equiv n + 6n_2 \bmod 12$.*

(b) *Assume $j = 0$. Then $a_2 = 0$ and $a_4 \neq 0$. Choose a square root $\sqrt{-a_4} \in \bar{K}$ and consider the field $\tilde{K} := K(\sqrt{-a_4})$. Set $n := v(a_6^2/a_4^3)$, $\tilde{n} := 2v^{*\tilde{K}}(a_6/a_4\sqrt{-a_4})$, and define $d' \in \{0, 3, 6, 9\}$ by $d' \equiv v(a_4^3) \bmod 12$.*

*Then $n \leq \tilde{n}$, and $n = \tilde{n}$ if $0 > n \equiv \pm 1 \bmod 3$.*
*Setting $\ell := \lfloor \frac{10 - d' - \tilde{n}}{12} \rfloor$, the invariants $d := d_v(E/K)$, $f := f_v(E/K)$, $m := m_v(E/K)$ and $\kappa := \kappa_v(E/K)$ are given by the following table.*

| $j \neq 0$ | | | $j = 0$ *or* $n \leq 0$ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $n > 0$ | | | $\tilde{n}$ | $\geq 0$ | | | | $< 0$ | | | |
| $n_2$ | *even* | *odd* | $d'$ | 0 | 3 | 6 | 9 | | | | |
| $d$ | $n$ | $n+6$ | $d$ | 0 | 3 | 6 | 9 | $12\ell + d'$ | | | |
| $f$ | 1 | 2 | $f$ | 0 | 2 | 2 | 2 | $2 - \tilde{n}$ | | | |
| $m$ | $n$ | $n+5$ | $m$ | 1 | 2 | 5 | 8 | 1 | 3 | 7 | 9 |
| $\kappa$ | $\mathrm{I}_n$ | $\mathrm{I}_n^*$ | $\kappa$ | $\mathrm{I}_0$ | III | $\mathrm{I}_0^*$ | $\mathrm{III}^*$ | II | IV | $\mathrm{IV}^*$ | $\mathrm{II}^*$ |

*In the last column, $m = 12\ell + d' + \tilde{n} - 1 \in \{1, 3, 7, 9\}$.*

**Proof** Let $e := (v(\tilde{K}^*) : v(K^*))$ be the ramification index in $\tilde{K}|K$. The extension $\tilde{K}|K$ is Kummer of degree 1 or 2, and we have $e = 1$ iff $n$ is even. By Proposition 1.5 and because $e \equiv \pm 1 \bmod 3$, we have $n \leq \tilde{n}$, and $n = \tilde{n}$ if $0 > n \equiv \pm 1 \bmod 3$. Furthermore we fix the notations $n_i := v(a_i)$, $L := K(E[2])$ and $G_s := G_s(L|K)$. Since $\tilde{K}|K$ is tamely ramified, we have $G_s = G_s(L|\tilde{K})$ for all $s \geq 1$. Note that $j = 0$ iff $a_2 = 0$.

(a) After the transformation $(1, a_4/a_2, 0, 0)$ (which does not affect $j$ nor $a_2$), we can assume that $a_4 = 0$. Then $a_6 \neq 0$, $j = -a_2^3/a_6$, and (the right hand side of) (2) has discriminant $\Delta := -a_2^3a_6 = a_2^6/j$, so $d \equiv v(\Delta) = n + 6n_2 \equiv d' \bmod 12$.

Let us first consider the case $n > 0$, *i.e.,* $3n_2 > n_6$. If $n_2$ is even, then after the transformation $(\pi^{n_2/2}, 0, 0, 0)$ we achieve $n_2 = 0$ and $n_6 > 0$. Entering this data into Tate's algorithm (see *e.g.,* [9, pp. 364–368]), in that algorithm's second step we find that $f = 1$, $m = n$ and $\kappa = \mathrm{I}_n$. Then $d = f + m - 1 = n$ by Ogg's Formula. If $n_2$ is odd, the transformation $(\pi^{(n_2-1)/2}, 0, 0, 0)$ leads to $n_2 = 1$, $n_6 > 3$, and here Tate's Algorithm renders $f = 2$, $m = n+5$ and $\kappa = \mathrm{I}_n^*$ in Step 7, whereupon Ogg's Formula yields $d = f + m - 1 = n + 6$. Thereby we have proved the left-hand side of the table.

Conversely, if $\kappa = \mathrm{I}_\nu$ or $\mathrm{I}_\nu^*$ with $\nu \geq 1$, then $n > 0$, also by Tate's Algorithm (see the table in [9, p. 365]). In fact, the former Kodaira type corresponds to multiplicative reduction, and $\mathrm{I}_\nu^*$ to a quadratic twist (by $\sqrt{\pi}$) of $I_\nu$. So, one must have $v(j) < 0$ by the semistable reduction criterion [8, p. 181]. Therefore, assuming $-n = v(j) \geq 0$ from now on, we know that $f \neq 1$ and $\kappa$ must be one of $\mathrm{I}_0$, II, III, IV, $\mathrm{I}_0^*$, IV$^*$, III$^*$, II$^*$.

Write $x^3 + a_2x^2 + a_6 = (x - x_1)(x - x_2)(x - x_3)$ with $x_i \in \bar{K}$. Then $E[2] = \{O, P_1, P_2, P_3\}$ where $P_i := (x_i, 0)$, and $L = K(x_1, x_2, x_3)$ is Galois over $K$ with group $G := G(L|K) \leq S_3$. Setting $\delta := (x_1-x_2)(x_2-x_3)(x_3-x_1) \in L$ we have that $\delta^2 = \Delta = a_6^2 j$, hence $\tilde{K} = K(\delta)$, and $G(L|\tilde{K}) = G \cap A_3$ is contained in the alternating group $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$. Therefore, after renumbering the $x_i$, we obtain $L = K(\delta, x_1) = \tilde{K}(x_1)$. Put $z := a_2/\sqrt{j}x_1$, then $L = \tilde{K}(z)$ and

$$z^3 - z = (a_2^3 - a_2 j x_1^2)/j\sqrt{j}x_1^3 = -(a_6 + a_2 x_1^2)/\sqrt{j}x_1^3 = 1/\sqrt{j}.$$

Now consider the case $n \leq 0 \leq \tilde{n}$. By Proposition 1.5, we must have $n \equiv 0 \bmod 3$, hence $d \equiv v(\Delta) = n + 6n_2 \equiv d' \equiv 0 \bmod 3$. Moreover, $L = \tilde{K}(z)$ is tamely ramified over $K$, hence $f = f_\nu^0(E/K) \leq 2$, *i.e.,* $f \in \{0, 2\}$. Thus $d = m + f - 1 \leq m + 1 \leq 10$ by Ogg's Formula and Table 1, so we have $d = d'$. Now, $d = 0$ is necessary and sufficient for $E/K$ to have good reduction, *i.e.,* $\kappa = \mathrm{I}_0$, $m = 1$ and $f = 0$. For $d' \neq 0$ we are left with $f = 2$ and obtain $m = d + 1 - f = d' - 1 = 2, 5, 8$ corresponding to $\kappa = \mathrm{III}, \mathrm{I}_0^*, \mathrm{III}^*$.

Let us finally consider the case $\tilde{n} < 0$. By Proposition 1.5, this means that $L|\tilde{K}$ is wildly ramified with the single jump $\tilde{s} = -e\tilde{n}/2 > 0$. Since $G_1 = G_{\tilde{s}} = G(\tilde{K}(x_1)|\tilde{K}) = A_3$ does not fix $P_1 = (x_1, 0)$, we must have $E[2]^{G_1} = \{O\}$. Noting that $|G_0| = 3e$, we compute

$$f_\nu^1(E/K) = \sum_{i=1}^{\tilde{s}} \frac{\dim_{\mathbb{F}_2} E[2]/E[2]^{G_i}}{(G_0 : G_i)} = \frac{2\tilde{s}}{e} = -\tilde{n}$$

and obtain $f = 2 - \tilde{n}$ from the definition of the conductor exponent and Proposition 1.2(b). Since $n < \tilde{n}$ iff $n \equiv 0 \bmod 3$, we have $n + \tilde{n} \equiv \pm 1 \bmod 3$ and Ogg's Formula yields

$$m = d + 1 - f \equiv n + 6n_2 + \tilde{n} - 1 \equiv n + \tilde{n} - 1 \equiv 0, 1 \bmod 3.$$

By Table 1, this means $m = 1, 3, 7, 9$, corresponding to $\kappa = \mathrm{II}, \mathrm{IV}, \mathrm{IV}^*, \mathrm{II}^*$. Writing $d = 12\ell + d'$ with $\ell \in \mathbb{N}_0$, we have $m = d + 1 - f = 12\ell + d' + \tilde{n} - 1 \in \{1, 3, 7, 9\}$, hence $\ell = \lfloor \frac{10 - d' - \tilde{n}}{12} \rfloor$.

(b) So $j = 0 = a_2$, (2) has discriminant $\Delta = -a_4^3 \neq 0$, and $d \equiv v(\Delta) = 3n_4 \equiv d' \bmod 12$. Note that again, since $j$ is integral, $E/K$ has potentially good reduction, that is, $\kappa$ is one of $\mathrm{I}_0$, II, III, IV, $\mathrm{I}_0^*$, IV$^*$, III$^*$, II$^*$, and $f \neq 1$.

Write $x^3 + a_4x + a_6 = (x - x_1)(x - x_2)(x - x_3)$ with $x_i \in \bar{K}$. Then $E[2] = \{O, P_1, P_2, P_3\}$ where $P_i := (x_i, 0)$, and $L = K(x_1, x_2, x_3)$ is Galois over $K$ with group $G := G(L|K) \leq S_3$. Setting $\delta := (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \in L$ we have that

$\delta^2 = \Delta = -a_4^3$, hence $\tilde{K} = K(\delta)$ and $G(L|\tilde{K}) = G \cap A_3$. Therefore, after renumbering the $x_i$, we obtain $L = K(\delta, x_1) = \tilde{K}(x_1)$. Put $z := x_1/\sqrt{-a_4}$, then $L = \tilde{K}(z)$ and

$$z^3 - z = (x_1^3 + a_4 x_1)/(-a_4\sqrt{-a_4}) = a_6/a_4\sqrt{-a_4}.$$

First consider the case $\tilde{n} \geq 0$. By Proposition 1.5, $L|K$ is tamely ramified hence $f \leq 2$, *i.e.,* $f \in \{0, 2\}$. Thus $d = m + f - 1 \leq m + 1 \leq 10$ by Ogg's Formula and Table 1, so we have $d = d'$. Now, $d = 0$ is necessary and sufficient for $E/K$ to have good reduction, *i.e.,* $\kappa = \mathrm{I}_0$, $m = 1$ and $f = 0$. For $d' \in \{3, 6, 9\}$, we are left with $f = 2$ and obtain $m = d+1-f = d'-1 = 2, 5, 8$ corresponding to $\kappa = \mathrm{III}, \mathrm{I}_0^*, \mathrm{III}^*$. The proof in case $\tilde{n} < 0$ is literally the same as in (a). ■

As a consequence, we can determine the possible conductor exponents and Kodaira types for each value of $v(j)$.

***Corollary 2.2*** *Let $\nu \in \mathbb{Z} \cup \{\infty\}$. Then*

(a) $\mathcal{F}_\nu = \{1, 2\}$ *for* $\nu < 0$,
(a′) $\mathcal{F}_0 = \{0, 2\}$,
(b) $\mathcal{F}_\nu = \{2 + \nu\}$ *for* $0 < \nu \equiv \pm 1 \bmod 3$,
(c) $\mathcal{F}_\nu = \{0 \leq f < 2 + \nu \mid f = 2 \text{ or } f \equiv 0, 4 \bmod 6\}$ *for* $0 < \nu \equiv 0 \bmod 6$,
(d) $\mathcal{F}_\nu = \{2 \leq f < 2 + \nu \mid f = 2 \text{ or } f \equiv 1, 3 \bmod 6\}$ *for* $0 < \nu \equiv 3 \bmod 6$,
(e) $\mathcal{F}_\infty = \{f \in \mathbb{N}_0 \mid f = 0 \text{ or } f = 2 \text{ or } 2 < f \not\equiv 2 \bmod 3\}$,

*and*

(a) $\mathcal{K}_\nu = \{\mathrm{I}_{-\nu}, \mathrm{I}_{-\nu}^*\}$ *for* $\nu \leq 0$,
(b) $\mathcal{K}_\nu = \{\mathrm{IV}, \mathrm{II}^*\}$ *for* $0 < \nu \equiv 1 \bmod 3$,
(b′) $\mathcal{K}_\nu = \{\mathrm{II}, \mathrm{IV}^*\}$ *for* $0 < \nu \equiv 2 \bmod 3$,
(c) $\mathcal{K}_\nu = \{\mathrm{I}_0, \mathrm{I}_0^*, \mathrm{II}, \mathrm{IV}, \mathrm{IV}^*, \mathrm{II}^*\}$ *for* $0 < \nu \equiv 0 \bmod 6$,
(d) $\mathcal{K}_3 = \{\mathrm{III}, \mathrm{III}^*, \mathrm{II}, \mathrm{IV}^*\}$,
(d′) $\mathcal{K}_\nu = \{\mathrm{III}, \mathrm{III}^*, \mathrm{II}, \mathrm{IV}, \mathrm{IV}^*, \mathrm{II}^*\}$ *for* $3 < \nu \equiv 3 \bmod 6$,
(e) $\mathcal{K}_\infty = \{\mathrm{I}_0, \mathrm{III}, \mathrm{I}_0^*, \mathrm{III}^*, \mathrm{II}, \mathrm{IV}, \mathrm{IV}^*, \mathrm{II}^*\}$.

**Proof** We take up the notations of Theorem 2.1. The assertions (a)– (b') and (e) follow easily from there. The actual work is to determine the possible values for $\tilde{n}$ in the case $0 < \nu = -n = v(j) \equiv 0 \bmod 3$.

Assume first $0 > n \equiv 0 \bmod 6$. Then $d' \in \{0, 6\}$, $\tilde{K}|K$ is unramified, and $\pi$ is a uniformizer for $\tilde{K}$. It follows that $\tilde{n} \in 2\mathbb{Z} \cup \{\infty\}$, hence either $\tilde{n} \in \{0, \infty\}$, or $n < \tilde{n} < 0$ with $\tilde{n} \equiv \pm 2 \bmod 6$. On the other hand, all these values for $d'$ and $\tilde{n}$ (except possibly $\tilde{n} = 0$) actually occur, as one sees by taking $a_2 \in \{1, \pi\}$ and $j = (\pi^{n/2} - \pi^{n/6} + \pi^{\tilde{n}/2})^{-2}$. (Here and below, we can include the case $\tilde{n} = \infty$ by the convention $\pi^\infty = 0$.) Looking at the corresponding cases in Theorem 2.1, (c) drops out.

Now consider the case $0 > n \equiv 3 \bmod 6$. Here $\tilde{\pi} := \pi^{(1-n)/2}/\sqrt{j}$ is a uniformizer in $\tilde{K}$, $\tilde{\pi}^2 = \pi^{1-n}/j$ is a new uniformizer for $K$, and $d' \in \{3, 9\}$. It follows that $1/\sqrt{j} \in \tilde{\pi}K \subseteq \tilde{\pi}k((\tilde{\pi}^2))$. Hence, either $\tilde{n} = \infty$, or $n < \tilde{n} < 0$ with $\tilde{n} \equiv \pm 1 \bmod 6$.

Again, all these values for $d'$ and $\tilde{n}$ occur, as one sees by taking $a_2 \in \{1, \pi\}$ and $j = (\tilde{\pi}^n - \tilde{\pi}^{n/3} + \tilde{\pi}^{\tilde{n}})^{-2} \in \mathbb{F}_3(\tilde{\pi}^2) \subseteq K$. Running through the respective cases in the theorem yields (d) and (d′). ∎

As Gekeler [3] already observed, the set of all possible conductor exponents (without any restrictions on $j$) equals

$$\mathcal{F} := \bigcup_{\nu \in \mathbb{Z} \cup \{\infty\}} \mathcal{F}_\nu = \{f \in \mathbb{N}_0 \mid f = 2 \text{ or } f \not\equiv 2 \bmod 3\} = \mathcal{F}_\infty \cup \{1\}.$$

All the above results concern a fixed valuation $v$ of $K$. But using weak approximation, we can prescribe the conductor exponent at any finite number of valuations on $K$.

***Corollary 2.3*** *Let $V$ be a finite set of discrete valuations on $K$ with perfect residue field. Then, given any $V$-tuple $(c_v)_{v \in V} \in \mathcal{F}^V$, there exists an elliptic curve $E/K$ such that $f_v(E/K) = c_v$ for all $v \in V$.*

## 3 Equal Characteristic 2

Throughout this section, we assume the characteristic of $K$ to be 2. Here, we shall only present a partial result, in that we do not treat the cases where $j = 0$ or $v(j)$ is positive and even.

***Theorem 3.1*** *Let $E/K$ be an elliptic curve with $j$-invariant $j := j(E) \neq 0$. Then $E/K$ can be given by a Weierstrass equation*

$$y^2 + xy = x^3 + a_2x^2 + a_4x + a_6. \tag{3}$$

*Moreover, we assume $v(j) \in \mathbb{Z} \setminus 2\mathbb{N}$. Set $n := v(1/j)$ and $n_2 := v^{*K}(a_2)$. Then the invariants $f := f_v(E/K)$, $d := d_v(E/K)$, $m := m_v(E/K)$ and $\kappa := \kappa_v(E/K)$ are given by the following table.*

| | $n = 0$ | $n > 0$ | $n < 0$ *odd or* $n \geq 0$ | $n < 0$ *odd* |
|---|---|---|---|---|
| | $n_2 \geq 0$ | $n_2 \geq 0$ | $n_2 < \min\{0, n/2\}$ | $n/2 \leq n_2 < n/3$ |
| $f$ | 0 | 1 | $2 - 2n_2$ | $2 - n$ |
| $d$ | 0 | $n$ | $n + 6 - 6n_2$ | $n + 6 - 6n_2$ |
| $m$ | 1 | $n$ | $n + 5 - 4n_2$ | $2n + 5 - 6n_2$ |
| $\kappa$ | $\mathrm{I}_0$ | $\mathrm{I}_n$ | $\mathrm{I}^*_{n-4n_2}$ | $\mathrm{I}^*_{2n-6n_2}$ |

| | $n < 0$ *and* $n_2 \geq n/3$ | | |
|---|---|---|---|
| $n$ mod 6 | 1 | 3 | 5 |
| $f$ | $2 - n$ | $2 - n$ | $2 - n$ |
| $d$ | $2 - n$ | $6 - n$ | $10 - n$ |
| $m$ | 1 | 5 | 9 |
| $\kappa$ | II | $\mathrm{I}^*_0$ | $\mathrm{II}^*$ |

**Proof** We may replace $K$ by its completion. Then $K = k((\pi))$ and $R = k[[\pi]]$. Starting from Equation (1), the transformation $(a_1, a_3/a_1, 0, 0)$ leads to the required form (3) with new coefficients $a_2, a_4, a_6 \in K$. After a subsequent transformation $(1, 0, s, a_4)$ with suitable $s \in K$ (which does not affect the definitions made) we may further assume that

$$a_4 = 0 \text{ and } a_2 \in \pi^{n_2} k[[\pi^2]], \tag{4}$$

in particular $n_2 = \nu(a_2)$. (Here we use the convention $\pi^\infty = 0$ again.) Our equation then has discriminant $\Delta = a_6 = 1/j$.

If $n, n_2 \geq 0$, then Tate's algorithm ends in Step 1 or 2, showing that our equation was already minimal and rendering the entries in our table's first two columns. For $n \leq \min\{0, 3n_2\}$, the transformation $(\pi^{\lfloor n/6 \rfloor}, 0, 0, 0)$ produces an integral equation, which we can feed into Tate's algorithm. If $n \equiv 1, 3, 5 \bmod 6$, then the algorithm terminates at Step 3, 6 and 10, respectively, showing that the integral equation was minimal and producing the last three columns of our table.

From now on, we concentrate on proving the remaining columns 3 and 4, thus assuming $n_2 < \min\{0, n/3\}$. Then again, the transformation $(\pi^{(n_2-1)/2}, 0, 0, 0)$ renders an integral equation, which when processed by Tate's algorithm, turns out to be minimal with $d = n + 6 - 6n_2$ and $\kappa = \mathrm{I}^*_{m-5}$, where $m$ or, equivalently, $f = d + 1 - m$ remains to be determined.

Write $E[3] = \{O, \pm P_1, \pm P_2, \pm P_3, \pm P_4\} \simeq \mathbb{F}_3^2$ with $P_i = (x_i, y_i)$. Then $-P_i = (x_i, y_i + x_i)$, and the $x_i$ are the roots of the third division polynomial

$$\psi = \psi_3 = x^4 + x^3 + \Delta = (x - x_1)(x - x_2)(x - x_3)(x - x_4),$$

the calculation of which is straightforward from the point addition formulas. Set $L := K(E[3])$, then $G := G(L|K)$ can be considered as a subgroup of $\mathrm{Aut}_{\mathbb{F}_3}(E[3]) \simeq \mathrm{GL}_2(\mathbb{F}_3)$. Obviously, the subfield fixed by $G \cap \{\pm 1\}$ is $L' := K(x_1, x_2, x_3, x_4)$, and $L = L'(y_i)$ for any $i$. Moreover, $G' := G(L'|K) \simeq G/G \cap \{\pm 1\}$ can be considered as a subgroup of $\mathrm{PGL}_2(\mathbb{F}_3) = \mathrm{GL}_2(\mathbb{F}_3)/\mathbb{F}_3^* \simeq S_4$, permuting the $x_i$. If we set

$$\rho := \sum_{\mu<\nu} \frac{x_\mu}{x_\mu + x_\nu} \quad \text{and} \quad \delta := \prod_{\nu_1<\nu_2<\nu_3} \sum_{i=1}^{3} \rho^{(-1)^{\nu_1+\nu_2+\nu_3} i} x_{\nu_i},$$

then a somewhat lengthy calculation renders

$$\rho^2 = \rho + 1 \text{ and } \delta^3 = \Delta.$$

This shows that $\tilde{K} := \mathbb{F}_4 K(\delta) \subseteq L'$. Moreover, for any $\sigma \in G' \leq S_4$, the definition of $\rho$ yields $\sigma(\rho) = \rho \iff \sigma \in A_4$, the alternating group. Hence $G(L'|\mathbb{F}_4 K) = G' \cap A_4$. Likewise, $G(L'|\tilde{K}) = G' \cap V_4$ from the definition of $\delta$, where $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ is the Klein 4-group sitting inside $A_4$. In particular, $[L' : \tilde{K}]$ divides 4. A short calculation shows that the monic degree 2 polynomials dividing $\psi$ are all of the form $g_u := x^2 + ux + u^3 + u^2$ with $u^3(u + 1)^3 = \Delta$. Since

$g_u g_{u+1} = \psi$ and $g_{u+1}(\frac{u+1}{u}x + u\rho + \rho) = \frac{u^2+1}{u^2} g_u(x)$, we conclude that $L' = \tilde{K}(x_i)$ for any $i$.

Choose $z \in \bar{K}$ with $z^4 + z = \delta$. Then $x_0 := z^3 + z^2 + z \neq 0$ and $\psi(x_0) = 0$, hence $x_0$ is one of the $x_i$. Let $y_0$ be a corresponding $y$-coordinate, that is $(x_0, y_0) \in E[3]$. Then $w := y_0/x_0$ satisfies

$$w^2 + w = x_0 + a_2 + \Delta/x_0^2 = a_2 + z^3 + \wp(x_0 + z) \text{ and } L = L'(w). \tag{5}$$

If we define $z_i := \rho^i z + \rho^{2i} z^2$ for $i = 0, 1, 2$, then

$$z_i^2 + z_i = \rho^i \delta, \quad z_0 = z_1 + z_2, \tag{6}$$

and $1 + \delta/x_0 = z = \rho z_1 + \rho^2 z_2$. Therefore, $L' = \tilde{K}(x_0) = \mathbb{F}_4 K(z) = K(z_1, z_2)$. The whole situation is illustrated in Figure 1.

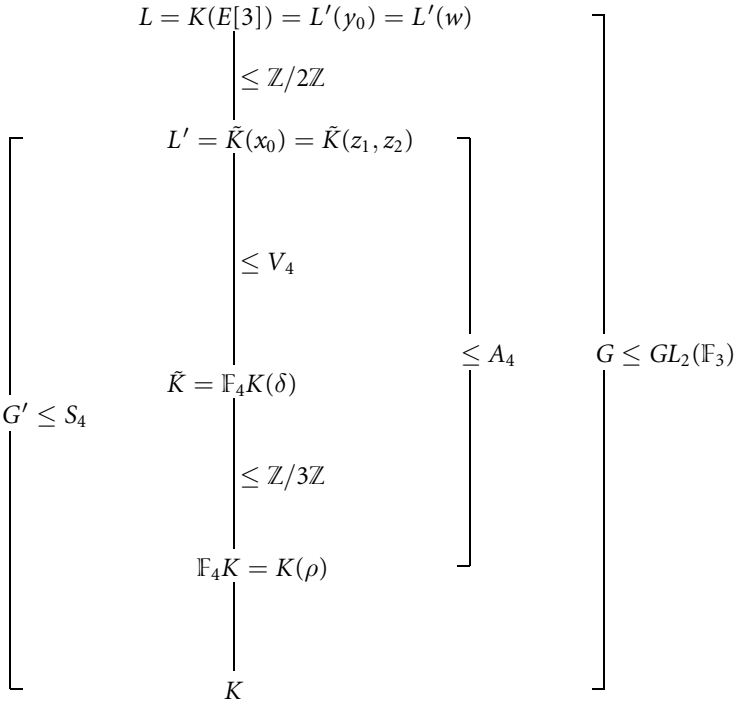


*Figure 1*: Subfields of $K(E[3])$

Set $G_s := G_s(L|K, v)$ and $\tilde{G}_s := G_s(L|\tilde{K}, v)$. Since $\tilde{K}|K$ is tamely ramified and $[L : \tilde{K}]$ divides 8, we have

$$(G_0 : G_1) = e := (v(\tilde{K}^*) : v(K^*)),\ G_1 = \tilde{G}_0, \text{ and } G_s = \tilde{G}_s \quad \forall s \geq 1. \tag{7}$$

Next we want to show that for all $s \geq 1$, one has either

$$G_s = 1 \text{ or } E[3]^{G_s} = \{O\}. \tag{8}$$

To this end, assume $\sigma \in \tilde{G}$ has a fixed point $\neq O$ in $E[3]$. Then $\sigma|_{L'} \in G(L'|\tilde{K}) \leq V_4$ must be trivial, i.e. $\sigma = \pm 1$. But $E[3]^{\{\pm 1\}} = \{O\}$, and so (8) is proven. Together with (7), we conclude

$$f^1 = f_v^1(E/K) = \frac{2}{e} \sum_{i=1}^{s_1} \frac{1}{(\tilde{G}_0 : \tilde{G}_i)} = 2\tilde{\eta}(s_1)/e, \tag{9}$$

where $s_1 := \max\{0, i \in \mathbb{N} \,|\, \tilde{G}_i \neq 1\}$ is the last jump of $L|\tilde{K}$, and $\tilde{\eta} := \eta_{L|\tilde{K}}$ is defined as in Chapter 1. If $n \geq 0$, then $L'|\tilde{K}$ is unramified. Hence, $s_1 = -ev^{*L'}(a_2 + z^3) = -en_2 > 0$ by (5), and $\tilde{\eta}$ is the identity on $[0, s_1]$. Substituting into (9) yields $f = 2 + f_1 = 2 - 2n_2$, whereby we proved the case $n \geq 0$ in our table's third column.

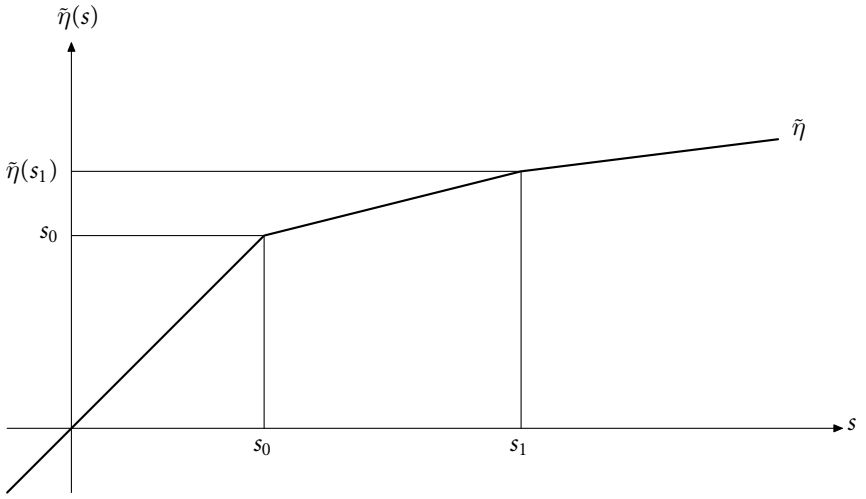


*Figure 2*: The graph of $\tilde{\eta}$

We are now left with the case $n_2 < n/3 < 0$. Using (6) and Proposition 1.5 and since $n$ is odd by assumption, $L' = K(z_1, z_2)$ is totally ramified of degree 4 over $\tilde{K}$ with the one jump $\tilde{s} = -ev^{*\tilde{K}}(\delta) = -en/3$. We shall show below that, under the current assumptions, we have

$$v^{*L'}(a_2) = n_2 - n/4. \tag{10}$$

Note that $v(z) = v(\delta)/4 = n/12$. Hence, by (5) and (10), and because $n$ is odd, $L|L'$ is (wildly) ramified with jump

$$\begin{aligned} s' &= -4ev^{*L'}(a_2 + z^3) = -4e\min\{n_2 - n/4, n/4\} \\ &= e\max\{-n, n - 4n_2\} \geq -en > \tilde{s}. \end{aligned}$$

By Proposition 1.1, $s_0 = \tilde{s} = -en/3$ is the first lower jump of $L|\tilde{K}$, $s_1 = s'$, and $\tilde{\eta}$ is the identity on $[-1, s_0]$ and has slope $1/4$ on $(s_0, s_1)$ (see Figure 2), so that we obtain

$$f = 2 + 2(s_0 + \tfrac{s_1 - s_0}{4})/e = 2 - \tfrac{n}{2} + \tfrac{s'}{2e} = \begin{cases} 2 - 2n_2 & \text{if } n_2 < n/2, \\ 2 - n & \text{if } n/2 \leq n_2 < n/3, \end{cases}$$

from (9) and Proposition 1.2, as desired. It remains to prove (10). To this end, let $\tilde{k}$ be the constant field of $\tilde{K}$ (and $L'$).

Let us first assume $n \equiv 3 \bmod 12$. Then $e = 1$, $\tilde{K} = \tilde{k}((\pi))$, and $\varpi := \pi^{(3-n)/12}z$ has valuation $v(\varpi) = 1/4$, hence $L' = \tilde{k}((\varpi))$. From $\pi^{1-n/3}/\varpi^4 = z^{-4} = (1 + z^{-3})/\delta$, we conclude $\pi = (\varpi^4 + \varpi^4/z^3)\pi^{n/3}/\delta \in \varpi^4\tilde{k}[[\pi]] + \varpi^{4-n}\tilde{k}[[\varpi]]$, hence

$$\tilde{k}[[\pi]] \subseteq \tilde{k}[[\varpi^4]] + \varpi^{4-n}\tilde{k}[[\varpi]]. \tag{11}$$

Now, $\pi^{n/3-1}\varpi^4 = z^4 = \delta + z$ implies $\pi^{-1} = \varpi^{-4}(1 + z/\delta)\delta/\pi^{n/3}$. Thus, using (11), we obtain for any odd $r \in \mathbb{N}$

$$\begin{aligned} \pi^{-r} &\in \varpi^{-4r}(1 + z/\delta)^r\tilde{k}[[\pi]]^* \subseteq \varpi^{-4r}\tilde{k}[[\varpi^4]] + \varpi^{-n-4r}\tilde{k}[[\varpi]]^* \\ &\subseteq \varpi^{-n-4r}\tilde{k}[[\varpi]]^* + \varpi^{-r}\tilde{k}[[\varpi]] + \wp L', \end{aligned}$$

so that (10) follows from (4) and because $n > 3n_2$. Similarly, if $n \equiv -3 \bmod 12$, then we can set $\varpi = \pi^{(3+n)/12}/z$, obtain (11) from $\pi^{1+n/3}/\varpi^4 = z^4 = \delta + z$ and derive (10) from $\pi^{-1-n/3}\varpi^4 = z^{-4} = (1 + z^{-3})/\delta$.

Now we turn to the cases where $n$ is not divisible by 3. Then $e = 3$ and $\tilde{k} = k$. If $n \equiv 1 \bmod 3$, then $\tilde{\pi} := \delta/\pi^{(n-1)/3}$ satisfies $v(\tilde{\pi}) = 1/3$ and $\tilde{\pi}^3 = \Delta/\pi^{n-1} \in K$. Likewise, if $n \equiv -1 \bmod 3$, then $\tilde{\pi} := \pi^{(n+1)/3}/\delta$ satisfies $v(\tilde{\pi}) = 1/3$ and $\tilde{\pi}^3 = \pi^{n+1}/\Delta \in K$. In both cases we can take $\tilde{\pi}$ as a uniformizer for $\tilde{K} = k((\tilde{\pi}))$, and replace the uniformizer $\pi$ of $K$ by $\tilde{\pi}^3$. Therefore, we may assume by (4) that

$$a_2 \in \tilde{\pi}^{3n_2}k[[\tilde{\pi}^6]]^* \tag{12}$$

Suppose that $n \equiv 1, 5 \bmod 12$. Then $\varpi := \tilde{\pi}^{(1-n)/4}z$ has valuation $v(\varpi) = 1/12$, hence $L' = k((\varpi))$. From $\tilde{\pi}^{1-n}/\varpi^4 = z^{-4} = (1 + z^{-3})/\delta$ we conclude

$$\tilde{\pi} = (\varpi^4 + \varpi^4/z^3)\tilde{\pi}^n/\delta \in \varpi^4 k[[\tilde{\pi}]] + \varpi^{4-3n}k[[\varpi]],$$

hence

$$k[[\tilde{\pi}]] \subseteq k[[\varpi^4]] + \varpi^{4-3n}k[[\varpi]]. \tag{13}$$

Now, $\tilde{\pi}^{n-1}\varpi^4 = z^4 = \delta + z$ implies $\tilde{\pi}^{-1} = \varpi^{-4}(1 + z/\delta)\delta/\tilde{\pi}^n$. Thus, using (13), we obtain for any odd $r \in \mathbb{N}$

$$\begin{aligned}\tilde{\pi}^{-r} &\in \varpi^{-4r}(1 + z/\delta)^r k[[\tilde{\pi}]]^* \subseteq \varpi^{-4r}k[[\varpi^4]] + \varpi^{-3n-4r}k[[\varpi]]^* \\ &\subseteq \varpi^{-3n-4r}k[[\varpi]]^* + \varpi^{-r}k[[\varpi]] + \wp L',\end{aligned}$$

so that (10) follows from (12) and because $n > 3n_2$. Similarly, if $n \equiv -1, -5 \bmod 12$, then we can set $\varpi = \tilde{\pi}^{(1+n)/4}/z$, obtain (13) from $\tilde{\pi}^{1+n}/\varpi^4 = z^4 = \delta + z$ and derive (10) from $\tilde{\pi}^{-1-n}\varpi^4 = z^{-4} = (1 + z^{-3})/\delta$. ∎

As a matter of convenience, in the following remark and example, we retain the notation of the previous theorem and its proof.

***Remark 3.2*** To determine the conductor exponent in general, we define

$$\tilde{N} := \{3v^{*\bar{K}}(\rho^i\delta) \mid i \in \mathbb{Z}\},$$

$$\tilde{n}_0 := \min \tilde{N},\ \tilde{n}_1 := \max \tilde{N},\ \text{and } n_2' := 12v^{*L'}(a_2 + z^3).$$

Then $n \le \tilde{n}_0, \tilde{n}_1 \in \mathbb{Z} \cup \{\infty\}$, $\min\{12n_2, 3n\} \le n_2' \in \mathbb{Z} \cup \{\infty\}$, and

$$f = \begin{cases} 0 \text{ or } 2 & \text{if } 0 \le \tilde{n}_0, n_2', \\ 2 - n_2'/6 & \text{if } n_2' < 0 \le \tilde{n}_0, \\ 2 - 2\tilde{n}_0/3 & \text{if } \tilde{n}_0 < 0 \le \tilde{n}_1 \text{ and } 2\tilde{n}_0 \le n_2', \\ 2 - \tilde{n}_0/3 - n_2'/6 & \text{if } n_2' \le 2\tilde{n}_0 < 0 \le \tilde{n}_1, \\ 2 - 2\tilde{n}_0/3 & \text{if } \tilde{n}_0 \le \tilde{n}_1 < 0 \text{ and } 2\tilde{n}_0 - \tilde{n}_1 \le n_2', \\ 2 - \tilde{n}_0/3 - \tilde{n}_1/6 - n_2'/6 & \text{if } n_2' \le 2\tilde{n}_0 - \tilde{n}_1 \le \tilde{n}_1 < 0. \end{cases}$$

These formulas can be obtained by drawing $\tilde{\eta}$ in a similar way as in the previous proof. Moreover, for even $n < 0$, the possible values of $\tilde{n}_0$ and $\tilde{n}_1$ are given as follows.

(a) If $n \equiv \pm 2 \bmod 12$, then $n < \tilde{n}_0 = \tilde{n}_1 < n/2$ with $\tilde{n}_0 \equiv n + 3 \bmod 6$, or $\tilde{n}_0 = \tilde{n}_1 = n/2$.

(b) If $n \equiv \pm 4 \bmod 12$, then $n < \tilde{n}_0 = \tilde{n}_1 < 0$ with $\tilde{n}_0 \equiv 3 - n/2 \bmod 6$, or $n/2 < \tilde{n}_0 = \tilde{n}_1 < 0$ with $\tilde{n}_0 \equiv n/2 - 3 \bmod 6$, or $\tilde{n}_0 = \tilde{n}_1 = \infty$.

(c) If $n \equiv 0 \bmod 6$, then $n < \tilde{n}_0 = \tilde{n}_1 < n/2$ or $n/2 \le \tilde{n}_0 \le \tilde{n}_1 \le \infty$, both with $\tilde{n}_0, \tilde{n}_1 \in (3 - 6\mathbb{N}) \cup \{0, \infty\}$.

The proofs for these facts are easy but lengthy and therefore omitted. Also, it is seen by simple examples that all these cases indeed occur (except for possibly $\tilde{n}_0, \tilde{n}_1 = 0$). ∎

Quite unlike the situation of the theorem, for even $n < 0$, the value of $n_2'$ does in general not depend on $n_2$, $n$, $\tilde{n}_0$ and $\tilde{n}_1$ alone. This drawback, which is the reason that we only presented a partial result, is illustrated in the following example.

***Example 3.3*** For the two elliptic curves over $K$ given below, we have $n_2 = -1$, $n = -4$ and $\tilde{n}_0 = \tilde{n}_1 = \infty$ but different values of $n_2'$.

(a)The elliptic curve

$$E : y^2 + xy = x^3 + \pi^{-1}x^2 + \pi^{-1} + \pi^{-2} + \pi^{-3} + \pi^{-4}$$

gives $n_2' = \infty$, $f = 2$, $m = 7$ and $\kappa = \mathrm{IV}^*$.
(b)The elliptic curve

$$E : y^2 + xy = x^3 + \rho\pi^{-1}x^2 + \pi^{-1} + \pi^{-2} + \pi^{-3} + \pi^{-4}$$

gives $n_2' = -12$, $f = 4$, $m = 5$ and $\kappa = \mathrm{I}_0^*$.
(In both cases, we can take $\tilde{\pi} := (1 + \pi^{-1})/\delta$ as a uniformizer for $\tilde{K} = K(\delta)$ which satisfies $\tilde{\pi}^3 = \pi$.)

We would expect similar (partial) results for the case $j = 0$, which (like in equal characteristic 3) would have to be treated separately in an analogous way. Let us conclude by writing down the possible conductor exponents and Kodaira types for the cases we did treat. The results follow directly from Theorem 3.1.

***Corollary 3.4*** *Let $\nu \in \mathbb{Z} \setminus 2\mathbb{N}$. Then*

(a) $\mathcal{F}_\nu = \{1\} \cup 4\mathbb{N}$ *for* $\nu < 0$,
(a′) $\mathcal{F}_0 = 4\mathbb{N}_0$,
(b) $\mathcal{F}_\nu = \{2 + \nu, f \mid 2 + \nu < f \equiv 0 \bmod 4\}$ *for* $0 < \nu$ *odd,*

*and*

(a) $\mathcal{K}_\nu = \{\mathrm{I}_{-\nu}, \mathrm{I}^*_{r-\nu} \mid 0 < r \equiv 4 \bmod 8\}$ *for* $\nu \leq 0$,
(b) $\mathcal{K}_\nu = \{\mathrm{I}^*_r \mid r \in 12\mathbb{Z} \cap [0, \nu]$ *or* $\nu < r \equiv 4 - \nu \bmod 8\}$ *for* $0 < \nu \equiv 3 \bmod 6$,
(b′) $\mathcal{K}_\nu = \{\mathrm{II}^*, \mathrm{I}^*_r \mid r \in (4 + 12\mathbb{Z}) \cap [0, \nu]$ *or* $\nu < r \equiv 4 - \nu \bmod 8\}$
*for* $0 < \nu \equiv 1 \bmod 6$,
(b″) $\mathcal{K}_\nu = \{\mathrm{II}, \mathrm{I}^*_r \mid r \in (8 + 12\mathbb{Z}) \cap [0, \nu]$ *or* $\nu < r \equiv 4 - \nu \bmod 8\}$
*for* $0 < \nu \equiv -1 \bmod 6$.

The union of the above sets $\mathcal{F}_\nu$ is $\bigcup_{\nu \in \mathbb{Z}\setminus 2\mathbb{N}} \mathcal{F}_\nu = \{f \in \mathbb{N}_0 \mid f \not\equiv 2 \bmod 4\}$. As Gekeler [3] has shown, the set of all possible conductor exponents equals

$$\mathcal{F} := \bigcup_{\nu \in \mathbb{Z} \cup \{\infty\}} \mathcal{F}_\nu = \mathbb{N}_0.$$

## References


[1] Roland Auer. *Ray Class Fields of Global Function Fields with Many Rational Places.* Thesis at the University of Oldenburg, Germany, 1999.
[2] E.-U. Gekeler, *Highly ramified pencils of elliptic curves in characteristic* 2. Duke Math. J. **89**(1997), 95–107.
[3] ———, *Local and global ramification properties of elliptic curves in characteristics two and three.* In: Algorithmic Algebra and Number Theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 49–64.
[4] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux.* Inst. Hautes Études Sci. Publ. Math. **21**(1964), 359–484.
[5] A. P. Ogg, *Elliptic curves and wild ramification.* Amer. J. Math. **89**(1967), 1–21.

[6] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3. J. Number Theory **44**(1993), 119–152.
[7] T. Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces.* Duke Math. J. **57**(1988), 151–173.
[8] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.
[9] ———, *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 151, Springer-Verlag, 1994.
[10] H. Stichtenoth, *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin, 1993.
[11] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In: Modular Functions of One Variable, IV, (Proc. Internat. Summer School Antwerp 1972, B. J.Birch, W. Kuyck, eds.). Lecture Notes in Math. 476, Springer, Berlin, 1975, pp. 33–52.

*Sternstr. 20*
*37083 Göttingen*
*Germany*
*e-mail: auer@math.usask.ca*

*IWI-RuG, P.O.Box 800*
*9700AV Groningen*
*The Netherlands*
*e-mail: top@math.rug.nl*